AMENDMENTS TO THE CLAIMS

1. (Currently Amended) A security communication packet processing apparatus that performs at least one of encryption processing, decryption processing and authentication processing ~~to~~ on an inputted packet so as to construct a processed packet corresponding to the inputted packet, said security communication packet processing apparatus comprising:

a control unit operable to divide the inputted packet into data blocks each having a B1 bit length, and sequentially output the data blocks obtained by the division, the B1 bit length being a unit of a data block on which one of the encryption processing and the decryption processing is performed;

at least one encryption processing unit operable to perform one of the encryption processing and the decryption processing ~~in a~~ on the data ~~block~~ blocks~~unit of B1 bits~~ outputted from said control unit;

at least one authentication processing unit operable to perform the authentication processing ~~in a data block unit of B2 bits~~ on data blocks each having a B2 bit length~~in parallel to the encryption processing or the decryption processing performed by said at least one encryption processing unit~~, and output an authentication value indicating the result of the authentication processing, the ~~data block unit of B2 bits~~ B2 bit length being a unit of a data block on which the authentication processing is performed and being n times the data block unit ~~of B1 bits~~ having the B1 bit length;

at least one data block accumulation unit operable to accumulate the data blocks each having the B1 bit length ~~to~~ on which the encryption processing has been performed by said at least one encryption processing unit, and, ~~when the amount of accumulated data blocks reaches B2 bits~~when the number of accumulated encrypted data blocks each having the B1 bit length reaches n, output the data ~~blocks~~ block having the B2 bit length made up of the n data blocks each having the B1 bit length, to said at least one authentication processing unit; and

a packet construction unit operable to receive the encrypted or decrypted data blocks from said at least one encryption processing unit, receive the authentication value from said at least one authentication processing unit, and ~~construct~~ reconstruct, according to a predetermined format, a processed packet corresponding to the inputted packet

~~including~~ by using the received data blocks and the authentication value; ~~and~~

~~a control unit operable to divide the inputted packet into the data blocks of B1 bits, and output the data blocks sequentially to said at least one encryption processing unit;~~

wherein when the inputted packet is a packet which requires both encryption processing and authentication processing, the encryption processing of ~~a first~~ the data block having the B1 bit length by said at least one encryption processing unit and the authentication processing of ~~a second~~ the data block having the B2 bit length by said at least one authentication processing unit are performed in parallel;~~, the second data block to which the authentication processing is being performed being a data block which is different from the first data block and to which the encryption processing has already been performed by said at least one encryption unit and accumulated in said at least one data block accumulation unit.~~

said at least one encryption processing unit is operable to generate encrypted data blocks by performing, one by one, the encryption processing on the data blocks each having the B1 bit length outputted, one by one, from said control unit, and output, one by one, the generated encrypted data blocks to said at least one data block accumulation unit and said packet construction unit;

said at least one data block accumulation unit is operable to accumulate the encrypted data blocks which have been outputted from said at least one encryption processing unit, and when the number of accumulated encrypted data blocks each having the B1 bit length reaches n, output the data block having the B2 bit length made up of the n encrypted data blocks each having the B1 bit length, to said at least one authentication processing unit;

said at least one authentication processing unit is operable to update an intermediate value obtained in the middle of generating the authentication value when said authentication processing unit receives the data block having the B2 bit length from said data block accumulation unit, using the data block having the B2 bit length, and output the intermediate value as the authentication value when said authentication processing unit updates the intermediate value using the at least one data block having the B2 bit length corresponding to the inputted packet; and

said packet construction unit is operable to (i) receive, from said at least one encryption processing unit, and accumulate, one by one, the encrypted data blocks corresponding to the data blocks obtained by dividing the inputted packet, (ii) receive the authentication value from said at least one authentication processing unit, and (iii) reconstruct the processed packet by using a set of the accumulated encrypted data blocks and the authentication value.

2. (Currently Amended) The security communication packet processing apparatus according to Claim 1, wherein:

said control unit is operable to judge whether the inputted packet is a first type packet requiring the encryption processing and the authentication processing, a second type packet requiring the decryption processing and the authentication processing, a third type packet requiring one of the encryption processing and the decryption processing, or a fourth type packet requiring the authentication processing only;

when said control unit judges that the inputted packet is the first type packet, said control unit is operable to divide the inputted packet into the data blocks ~~of B1 bits~~ each having the B1 bit length and output the divided data blocks each having the B1 bit length sequentially to said at least one encryption processing unit;

when said control unit judges that the inputted packet is the second type packet, said control unit is operable to divide the inputted packet into the data blocks ~~of B1 bits~~ each having the B1 bit length, output the divided data blocks ~~of B1 bits~~ each having the B1 bit length sequentially to said encryption processing unit, divide the inputted packet or a duplicate of the inputted packet into the data blocks ~~of B2 bits~~ each having the B2 bit length, and output the divided data blocks ~~of B2 bits~~ each having the B2 bit length sequentially to said at least one authentication processing unit;

when said control unit judges that the inputted packet is the third type packet, said control unit is operable to divide the inputted packet into the data blocks ~~of B1 bits~~ each having the B1 bit length and output the divided data blocks each having the B1 bith length sequentially to said at least one encryption processing unit; and

when said control unit judges that the inputted packet is the fourth type packet, said control unit is operable to divide the inputted packet into the data blocks ~~of B2 bits~~

each having the B2 bit length and output the divided data blocks each having the B2 bit length sequentially to said at least one authentication processing unit.

3. (Previously Presented) The security communication packet processing unit according to Claim 1, wherein:

the number of at least one of said at least one encryption processing unit and said at least one authentication processing unit is two or more; and

the number of said at least one data block accumulation unit is equal to the number of said at least one encryption processing unit.

4. (Previously Presented) The security communication packet processing apparatus according to Claim 3, wherein said control unit is operable to specify, among two or more encryption processing units or two or more authentication processing units, said encryption processing unit or said authentication processing unit that is ready for processing, and output the data blocks to the specified encryption processing unit or authentication processing unit.

5. (Previously Presented) The security communication packet processing apparatus according to Claim 1, further comprising a data path connection switching unit operable to connect the output of said control unit and the input of said at least one encryption processing unit, the output of said control unit and the input of said at least one authentication processing unit, the output of said at least one encryption processing unit and the input of said at least one data block accumulation unit, and the output of said at least one data block accumulation unit and the input of said at least one authentication processing unit, respectively and independently.

6. (Currently Amended) The security communication packet processing apparatus according to Claim 5, wherein:

said control unit is operable to judge whether the inputted packet is a first type packet requiring the encryption processing and the authentication processing, a second type packet requiring the decryption processing and the authentication processing, a third

type packet requiring one of the encryption processing and the decryption processing, or a fourth type packet requiring the authentication processing only;

when said control unit judges that the inputted packet is the first type packet, said control unit is operable to control said data path connection switching unit so as to connect the output of said control unit and the input of said at least one encryption processing unit, the output of said at least one encryption processing unit and the input of said at least one data block accumulation unit, and the output of said at least one data block accumulation unit and the input of said at least one authentication processing unit;

when said control unit judges that the inputted packet is the second type packet, said control unit is operable to control said data path connection switching unit so as to connect the output of said control unit and the input of said at least one encryption processing unit, and the output of said control unit and the input of said at least one authentication processing unit;

when said control unit judges that the inputted packet is the third type packet, said control unit is operable to control said data path connection switching unit so as to connect the output of said control unit and the input of said at least one encryption processing unit; and

when said control unit judges that the inputted packet is the fourth type packet, said control unit is operable to control said data path connection switching unit so as to connect the output of said control unit and the input of said at least one authentication processing unit.

7. (Previously Presented) The security communication packet processing apparatus according to Claim 6, wherein:

the number of at least one of said at least one encryption processing unit and said at least one authentication processing unit is two or more; and

the number of said at least one data block accumulation unit is equal to the number of said at least one encryption processing unit.

8. (Previously Presented) The security communication packet processing apparatus according to Claim 7, wherein said control unit is operable to specify, among two or more

encryption processing units or two or more authentication processing units, said encryption processing unit or said authentication processing unit that is ready for processing, and make said data path connection switching unit perform a connection for the specified encryption processing unit or authentication processing unit.

9. (Currently Amended) The security communication packet processing apparatus according to Claim 1, further comprising a processing data saving unit provided for each of at least one of said at least one encryption processing unit, said at least one authentication processing unit and said at least one data block accumulation unit, each processing data saving unit having a memory area, for each processing unit for which said processing data saving unit is provided, for temporarily suspending the processing of ~~the~~ at least one data ~~blocks~~ block in the processing unit ~~for which said processing data saving unit is provided~~, and saving the data ~~blocks~~ block which ~~were~~ was being processed in the processing unit ~~corresponding respectively to the processing unit~~.

10. (Currently Amended) The security communication packet processing apparatus according to Claim 9, wherein said control unit is operable to specify the processing unit that is performing the processing of the data ~~blocks~~ block of the inputted packet ~~with~~ having the lowest priority among the processing units, and, after suspending the processing of the data ~~blocks~~ block in the processing unit and saving the data ~~blocks~~ block which ~~were~~ was being processed in the processing unit into said processing data saving unit provided to the processing unit performing the processing of the data ~~blocks~~ block of the inputted packet ~~with~~ having the lowest priority, make the processing unit perform the processing of the data ~~blocks~~ block of ~~the~~ another inputted packet.

11. (Previously Presented) The security communication packet processing apparatus according to Claim 10, further comprising a data path connection switching unit operable to connect the output of said control unit and the input of said at least one encryption processing unit, the output of said control unit and the input of said at least one authentication processing unit, the output of said at least one encryption processing unit and the input of said at least one data block accumulation unit, and the output of said at

least one data block accumulation unit and the input of said at least one authentication processing unit, respectively and independently.

12. (Previously Presented) The security communication packet processing apparatus according to Claim 11, wherein:

the number of at least one of said at least one encryption processing unit and said at least one authentication processing unit is two or more; and

the number of said at least one data block accumulation unit is equal to the number of said at least one encryption processing unit.

13. (Currently Amended) The security communication packet processing apparatus according to Claim 1, further comprising a processing data saving unit provided for each of at least two of said at least one encryption processing unit, said at least one authentication processing unit and said at least one data block accumulation unit, each processing data saving unit having a memory area shared by the processing ~~units~~ unit for temporarily suspending the processing of ~~the~~ at least one data ~~blocks~~ block in the processing unit and saving the data ~~blocks~~ block which ~~were~~ was being processed in the processing ~~units~~unit.

14. (Currently Amended) The security communication packet processing apparatus according to Claim 13, wherein said control unit is operable to specify, among the processing units, the processing unit that is performing the processing of the data ~~blocks~~ block of the inputted packet ~~with~~ having the lowest priority, and, after suspending the processing of the data ~~blocks~~ block in the processing unit and saving the data ~~blocks~~ block which ~~were~~ was being processed in the processing unit in said processing data saving unit provided to the processing unit performing the processing of the data ~~blocks~~ block of the inputted packet ~~with~~ having the lowest priority, make the processing unit perform the processing of the data ~~blocks~~ block of ~~the~~ another inputted packet.

15. (Previously Presented) The security communication packet processing apparatus according to Claim 14, further comprising a data path connection switching unit operable

to connect the output of said control unit and the input of said at least one encryption processing unit, the output of said control unit and the input of said at least one authentication processing unit, the output of said at least one encryption processing unit and the input of said at least one data block accumulation unit, and the output of said at least one data block accumulation unit and the input of said at least one authentication processing unit, respectively and independently.

16. (Previously Presented) The security communication packet processing apparatus according to Claim 15, wherein:

the number of at least one of said at least one encryption processing unit and said at least one authentication processing unit is two or more; and

the number of said at least one data block accumulation unit is equal to the number of said at least one encryption processing unit.

17. (Previously Presented) The security communication packet processing apparatus according to Claim 1, wherein the B1 is 64, and the B2 is 512.

18. (Currently Amended) A security communication packet processing method ~~that performs~~for performing at least one of encryption processing, decryption processing and authentication processing ~~to~~ on an inputted packet so as to construct a processed packet corresponding to the inputted packet, said security communication packet processing method comprising:

dividing the inputted packet into data blocks ~~of B1 bits~~ each having a B1 bit length, and sequentially outputting the data blocks obtained by said dividing, the B1 bit length being a unit of a data block on which one of the encryption processing and the decryption processing is performed;

performing the encryption processing or the decryption processing ~~to the divided data blocks of B1 bits~~ on the data blocks outputted in said outputting;

~~accumulating the encrypted data blocks and outputting the data blocks when the amount of accumulated data blocks reaches B2 bits, B2 bits being n times the number of B1 bits;~~

performing the authentication processing ~~to the outputted data blocks of B2 bits in parallel to the encryption processing or the decryption processing~~ on data blocks each having a B2 bit length, and outputting ~~the~~ an authentication value indicating the result of the authentication processing, the B2 bit length being a unit of a data block on which the authentication processing is performed and being n times the data block having the B1 bit length;

accumulating the data blocks each having the B1 bit length on which the encryption processing has been performed in said performing of the encryption processing, and when the number of accumulated encrypted data blocks each having the B1 bit length reaches n, outputting the data block having the B2 bit length made up of the n data blocks each having the B1 bit length so that the data block the having the B2 bit length is processed in said performing of the authentication processing;

receiving the ~~encrypted or decrypted~~ data blocks encrypted or decrypted in said performing of the encryption processing or said performing of the decryption processing, receiving the ~~outputted~~ authentication value outputted in said outputting of the authentication value, and ~~constructing~~ reconstructing, according to a predetermined format, a processed packet corresponding to the inputted packet by using ~~the packet including~~ the received data blocks and the authentication value~~;~~, wherein:

~~wherein~~ when the inputted packet is a packet which requires both encryption processing and authentication processing, the encryption processing of ~~a first~~ the data block having the B1 bit length performed in said performing of the encryption processing and the authentication processing of ~~a second~~ the data block having the B2 bit length performed in said performing of the authentication processing are performed in parallel~~, the second data block to which the authentication processing is being performed being a data block which is different from the first data block and to which the encryption processing has already been performed in said performing of the encryption processing and accumulated in said accumulating of the encrypted data blocks.~~

in said performing of the encryption processing, encrypted data blocks are generated by performing, one by one, the encryption processing on the data blocks each having the B1 bit length outputted one by one in said outputting of the data blocks, and the generated encrypted data blocks are outputted one by one so that the data blocks are

processed in both of i) said accumulating of the data blocks each having the B1 bit length and outputting of the data block having the B2 bit length, and ii) said reconstructing of the processed packet;

in said accumulating of the data blocks each having the B1 bit length and outputting of the data block having the B2 bit length, the encrypted data blocks which have been outputted in said performing of the encryption processing are accumulated, and when the number of accumulated encrypted data blocks each having the B1 bit length reaches n, the data block having B2 the bit length made up of the n encrypted data blocks each having the B1 bit length is outputted so that the data block having the B2 bit length is processed in said performing of the authentication processing;

in said performing of the authentication processing, an intermediate value obtained in the middle of generating the authentication value is updated using the data block having the B2 bit length, when the data block having the B2 bit length accumulated in said accumulating is received, and the intermediate value is outputted as the authentication value when the intermediate value is updated using the at least one data block having the B2 bit length corresponding to the inputted packet; and

in said reconstructing, (i) the encrypted data blocks obtained in said performing of the encryption processing and corresponding to the data blocks obtained by dividing the inputted packet are received and accumulated one by one, (ii) the authentication value generated in said generating of the authentication value is received, and (iii) the processed packet is reconstructed by using a set of the accumulated encrypted data blocks and the authentication value.

19. (Currently Amended) The security communication packet processing method according to Claim 18, ~~further comprising~~wherein:

said dividing of the inputted packet comprises judging whether the inputted packet is a first type packet requiring the encryption processing and the authentication processing, a second type packet requiring the decryption processing and the authentication processing, a third type packet requiring only one of the encryption processing and the decryption processing, or a fourth type packet requiring the authentication processing only~~;~~ and

when the inputted packet is judged to be the first type packet, said method causes ~~controlling so that~~ the division in said dividing of the inputted packet, the encryption processing performed in said performing of the encryption processing or the decryption processing, the accumulation in said accumulating of the encrypted data blocks, the authentication processing performed in said performing of the authentication processing, and the construction performed in said constructing of the packet ~~are~~ to be performed.

20. (Previously Presented) The security communication packet processing apparatus according to claim 5, wherein said data path connection switching unit is operable to switch a data path between two of said control unit, said at least one encryption processing unit, said at least one authentication processing unit and said at least one data block accumulation unit, so that only packets A pass through said at least one data block accumulation unit and only packets B bypass said at least one data block accumulation unit, the packets A being a packet which requires both encryption processing and authentication processing and a packet which requires both decryption processing and authentication processing, and the packets B being a packet which requires only encryption processing, a packet which requires only decryption processing and a packet which requires only authentication processing.

21. (Currently Amended) The security communication packet processing apparatus according to claim 9, wherein the at least one data ~~blocks~~ block is ~~are~~ saved from said at least one encryption processing unit and said at least one authentication processing unit into said processing data saving unit, and the saved data ~~blocks~~ block is ~~are~~ restored from said processing data saving unit to the said at least one encryption processing unit and said at least one authentication processing unit, via said at least one data block accumulation unit.

22. (Currently Amended) The security communication packet processing apparatus according to claim 14, wherein said control unit is further operable to make another processing unit read the data ~~blocks~~ block from said processing data saving unit and restart the processing, the another processing unit having a function equivalent to a

function of the processing unit performing the processing of the data ~~blocks~~ block of the inputted packet with the lowest priority, from which processing unit the data ~~blocks~~ block ~~are~~ is saved into said processing data saving unit.